Bloomberg BNA

Privacy and Security Law Report®

Future Model: Florida's Progressive Data Breach Law



By Eduard Goodman, Ana Tagvoryan and Joshua Briones

Forty-seven states, four districts/territories (District of Columbia, Guam, Puerto Rico and the U.S. Virgin Islands) and one federal breach notification requirement under the Health Insurance Portability and Accountability Act have their own version of a breach notification law. California, for instance, has a five-day reporting requirement for in-state entities when there is a breach. Texas passed a comprehensive law in 2013 affecting folks both inside and outside the state. Massachusetts has a more comprehensive breach law that goes beyond simply addressing notifications. Wisconsin has a more stringent law relating to misdirected faxes, and Minnesota is rumored to be considering laws based on the California system. Many other states have other variations.[1]

With so many states doing so many different things, it may be time for Congress to consider passing a single breach notification law that levels the playing field to protect consumer privacy for businesses that accept sensitive, personally identifiable information. Florida's new law, the Florida Information Protection Act (FIPA), which went into effect July 1, so fundamentally changes what information is protected and to whom the law applies that it could serve as a model for a comprehensive congressionally, approved federal statute.[2] In addition, until such time as federal legislation is enacted, FIPA may very well serve as a model for other states to follow.

For these reasons, even if FIPA does not impact your business, we believe it is important to be familiar with key aspects of the law.

Reasonable Data Protection and Secure Disposal of Personal Information

FIPA requires that companies and government entities maintaining personal information of state residents

[1] Many different states have different definitions for what constitutes:

- private information: Arkansas (Ark. Code Ann. § 4-110-101 *et seq.*); California (Cal. Civ. Code §§ 1798.29, 1798.80 *et seq.*); Delaware (Del. Code Ann. tit. 6, § 12B-101 *et seq.*); Missouri (Mo. Rev. Stat. § 407.1500); Texas (Tex. Bus. & Com. Code Ann. §§ 521.002, 521.053; Tex. Educ. Code Ann. § 37.007(b)(5)); Virginia (Va. Code Ann. §§ 18.2-186.6, 32.1-127.1:05); Puerto Rico (if covered under HIPAA) (P.R. Laws Ann. tit. 10, § 4051 *et seq.*);
- biometric data (iris scan, fingerprint, etc.): Iowa (*see* Iowa Code §§ 715C.1, 715C.2); Nebraska (*see* Neb. Rev. Stat. §§ 87-801, 802–807); North Carolina (*see* N.C. Gen. Stat §§ 75-61, 75-65); Wisconsin (*see* Wis. Stat. § 134.98);
- miscellaneous information: Puerto Rico (work-related evaluations) (*see* P.R. Laws Ann. tit. 10, § 4051 *et seq.*); Oregon (passport number or other U.S.-issued identification number) (*see* Oregon Rev. Stat. § 646A.600 *et seq.*); North Dakota (date of birth, mother's maiden name, employee ID number, scanned or digital signature) (*see* N.D. Cent. Code § 51-30-01 *et seq.*); New York (any information concerning a natural person which because of name, number, personal mark or other identifier can be used to identify such natural person) (*see* N.Y. Gen. Bus. Law § 899-aa; N.Y. State Tech. Law § 208); and
- paper records: Alaska (*see* Alaska Stat. § 45.48.010 *et seq.*); Hawaii (*see* Haw. Rev. Stat. § 487N-1 *et seq.*); Indiana (*see* Ind. Code §§ 4-1-11 *et seq.*, 24-4.9 *et seq.*); North Carolina (*see* N.C. Gen. Stat §§ 75-61, 75-65); Iowa (has expanded its notification requirements to include paper records effective July 1) (*see* Iowa Code §§ 715C.1, 715C.2).

[2] 2014 Fla. Laws ch. 189, *available at* http://laws.flrules.org/2014/189 (13 PVLR 1168, 6/30/14); *see also* 2014 Fla. Laws. ch. 190 (codified as amended at Fla. Stat. § 501.171), *available at* http://laws.flrules.org/2014/190.

 ISSN 1538-3423

take steps to protect against data breaches through data security measures as well as secure disposal of personal information. Specifically, the act requires ''reasonable measures to protect and secure data in electronic form containing personal information,'' as well as ''reasonable measures to dispose . . . of customer records containing personal information within its custody or control when the records are no longer to be retained.'' FIPA specifies that such secure disposal ''shall involve shredding, erasing, or otherwise modifying personal information in the records to make it unreadable or undecipherable through any means.''

Expanded Notification Trigger From 'Unauthorized Acquisition' to 'Unauthorized Access'

FIPA expands the definition of ''breach'' from ''unlawful and unauthorized acquisition'' of personal information to ''unauthorized access'' of such information. This means notification obligations are triggered by ''unauthorized access'' alone. Thus, incidents which involve ''unauthorized access'' to, but not ''unauthorized acquisition'' of, personal information may trigger notification obligations.

Notification Requirements

FIPA includes the most comprehensive set of breach notification requirements for both covered entities and business associates as defined by HIPAA. Notification requirements are based on the number of individuals impacted. When 500 or more individuals are impacted, notification must be made to the state attorney general (AG) and to all individuals involved. For breaches affecting more than 1,000 individuals, the entity must notify all credit agencies in addition to the AG and individuals involved. Breaches involving fewer than 500 records require notifications only to the individuals affected. Covered entities are responsible for the actions of their subcontractors and agents.

Furthering the Trend—Expanded Definition of Personal Information

FIPA, adopting a common trend among states toward a more expansive definition of personal information, expands the definition of ''personal information'' to include an individual's first name or first initial and last name in combination with: (1) any information regarding the individual's medical history, mental or physical condition or medical treatment or diagnosis by a healthcare professional; or (2) the individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual. With respect to covered entities and business associates subject to HIPAA, compliance with the HIPAA breach notification rule[3] would appear to satisfy the requirements of the act, provided that the breached entity provides a copy of its HIPAA-compliant notifications to the Florida AG in a ''timely'' manner.

30-Day Deadline for Notifying Affected Individuals

FIPA reduces the deadline for notifying affected individuals from 45 to 30 days after discovery, requiring notice ''as expeditiously as practicable and without unreasonably delay . . . but no later than 30 days after determination of a breach or reason to believe a breach occurred,'' subject to law enforcement delay and risk of harm consultation exceptions.

Without proper planning, compliance here could present a challenge. For instance, the turnaround on a print run of 5,000-10,000 plus letters to affected individuals takes approximately five business days. Performing forensics analysis and/or related investigations could take between 36 hours to a week before accurate results could be reported. While most breaches may be responded to in one to two weeks after discovery, for those breaches that require thorough investigation and forensics, complying within 30 days may not be practical in light of current technologies. Thankfully, the act permits the AG to grant breached entities an additional 15 days to notify affected individuals if good cause for delay is provided to the AG in writing within 30 days after determination of the breach or reason to believe a breach occurred.

While certain industry-specific deadlines for notifying affected individuals are significantly shorter (e.g., notice to patients pursuant to the California medical breach notification statute is required within five business days of discovery[4]), most general state breach notification requirements do not specify the number of days within which notice is required, instead providing that notice is required ''as expeditiously as possible,'' ''without unreasonable delay'' or similar language. Certain other states require notification to affected individuals within 45 days of discovery, but breached entities may now need to respond more quickly to breaches affecting residents of Florida (including 50-state breaches), increasing the importance of an effective incident response plan.

Importantly, Florida is one of a small, growing number of jurisdictions and laws (HIPAA included) where businesses can provide notice electronically. The relevant law permits ''[e]-mail notice sent to the e-mail address of the individual in the records of the covered entity.'' This is significant because it allows businesses to proactively prepare for a breach by obtaining prior express consent from your patients, customers and clients to receive notifications electronically. This minimizes costs because when a breach occurs a company can avoid the expense of mailing 10,000 letters at $2.00 per letter via the U.S. Postal Service (with printing, database checks, return mail, postage, etc.). More and more people rely on electronic communications/notices and fewer and fewer on snail mail.

Production of Forensic Reports, Policies Regarding Breaches and Other Documentation to Attorney General

FIPA imposes unusual requirements to provide copies of the following documents to the AG upon request: ''a police report, incident report, or computer forensics report,'' and ''a copy of the policies in place regarding breaches.''

This requirement is perhaps the most controversial because *many* breaches are never reported to the police and because the nature of the breach never results in a forensic report. For instance, in one case in which digital photocopiers were loaded with alleged sensitive, personally identifiable information and reported by the CBS Evening News, no police or incident report was

[3] 45 C.F.R. §§ 164.400-164.414.

[4] Cal. Health & Safety Code § 1280.15(b)(1).

  PVLR ISSN 1538-3423

generated.[5] Smaller breaches will similarly not justify generating a forensic report or a police report. For example, when an attachment containing personal information is sent to the wrong recipients, data on a File Transfer Protocol (FTP) server that should have been on a Secure File Transfer Protocol (SFTP) server is instead indexed by Google or a company incorrectly mails W2 forms to individuals in a state that requires paper records, law enforcement officials are unlikely to generate a police report because there is no ''theft'' in the traditional sense. In many cases, therefore, it will not be possible to provide the requested reports, and the company will need to see whether the AG is satisfied on a case-by-case basis.

Penalties

FIPA, like HIPAA, stipulates civil monetary penalties, but unlike HIPAA, Florida's penalties are rolled out on a much different schedule. They are initially assessed daily, then weekly—and finally, there is an annual limit of $500,000.

As with many other state data breach statutes, FIPA can only be enforced by the state. Individuals do not have the right to sue for damages under FIPA because the statute does not create a private right of action. Whether a federal version will have this same feature, when many other federal statutes such as the Telephone Consumer Protection Act, Children's Online Privacy Protection Act and Video Privacy Protection Act (among others) create a private right to sue, remains to be seen.

[5] Armen Keteyian, *Digital Photocopiers Loaded With Secrets*, CBS (Apr. 29, 2010), http://www.cbsnews.com/news/digital-photocopiers-loaded-with-secrets/.

Concluding Remarks

As an immediate response to FIPA, businesses that collect personal information of individuals ''in Florida'' should prepare or update their incident response plans and consider implications of the forensic report disclosure requirement with respect to intentions to assert attorney-client privilege over forensic reports.

In light of the progressive and comprehensive nature of FIPA, other states may follow suit. FIPA may also encourage Congress to enact a common breach notification law modeled after it so that there are no longer multiple versions across different states.

Eduard Goodman is the chief privacy officer for IDentity Theft 911 LLC (IDT911) where he applies his knowledge and experience in international privacy, data protection and emerging technologies law to create insurance products and solutions geared toward small- to medium-size business risks. He also heads up IDT911's data breach response management team.

Ana Tagvoryan, a partner at Blank Rome LLP's Los Angeles office, handles a wide variety of privacy, social media and unfair competition matters in federal and state courts of California. She is a member of the firm's Corporate Litigation practice, with a focus on class action defense.

Joshua Briones, who is also a partner at Blank Rome's Los Angeles office, advises clients regarding compliance with state and federal laws that govern the use and disclosure of consumer information. He is a member of the firm's Corporate Litigation practice, with a focus on class action defense.

NEW PORTFOLIOS & TREATISES NOW AVAILABLE

SAFE DATA & SOUND SOLUTIONS

Privacy & Data Security Law Resource Center™

Unparalleled news. Expert analysis from the new Privacy & Data Security Portfolio Practice Series. Comprehensive new treatises. Proprietary practice tools. State, federal, and international primary sources. The all-in-one research solution that today's professionals trust to navigate and stay in compliance with the maze of evolving privacy and data security laws.

TO START YOUR FREE TRIAL CALL 800.372.1033 OR GO TO www.bna.com/privacy-insights

Bloomberg BNA